UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/786,756	06/20/2001	Erik Knudsen	KNUDSEN2	5096

1444 7590 02/11/2005

BROWDY AND NEIMARK, P.L.L.C.
624 NINTH STREET, NW
SUITE 300
WASHINGTON, DC 20001-5303

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 02/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/786,756	KNUDSEN, ERIK	
	Examiner	Art Unit	
	Michael J Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☒ Claim(s) *1-5,7,9 and 10* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/9/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The IDS of 3/9/01 was received and considered.

2. The preliminary amendment of 6/20/01 was received and considered.

3. Claims 1-10 are pending.

Specification

4. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

5. The spacing of the lines of the specification is such as to make reading and entry of amendments difficult. New application papers with lines double spaced on good quality paper are required. Some equation subscripts and superscripts are also not legible.

Claim Objections

6. The claims are objected to because some equation subscripts and superscripts are not legible. Substitute claims with legible equations are required. See 37 CFR 1.52(b).

7. Claim 1 is objected to because "the addition of points is an operation known in the art" does not appear to be a valid claim limitation.

8. Claims 2-5, 7 & 9-10 contain no-alphabetic/numeric bullets and dashes "-" to separate method steps inconsistent with standard practice. The claims should be written in single sentence form and the method steps should be clearly separated with semicolons, commas, etc. consistent with standard practice.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

10. Claims 1-10 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. An "odd order point" is not defined in the specification.

11. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

12. Claims 1-10 appear to be a translation and as such are not written in a form consistent with common U.S. practice. The method steps are considered to be performed in order.

13. Claims 2-3 are indefinite, because the limitation "if not, add x to said second value ... to calculate said halving" implies that the directly preceding operation is performed, however, it is not explicit. *For the purposes of this Office Action, "to calculate" is understood to mean "and calculate the halving...."*

14. Claims 2-3 are indefinite, because the second recitation of the limitation "if not, add x to said second value ... to calculate said halving as in the preceding operation" does not specify whether the preceding halving operation is the first halving or the second halving. *For the purposes of this Office Action, "the preceding operation" is understood to mean "the directly preceding operation".*

15. Claims 6-7 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

16. Claim 6 is indefinite because it is unclear what 'it' (line 2) is referring to. *For the purposes of this Office Action, 'it' is understood to refer to "the method" of claim 1.*

17. Claim 6 provides for the use of the method of claim 1, but, since the claim does not set forth any steps involved in the method/process, it is unclear what method/process applicant is intending to encompass. A claim is indefinite where it merely recites a use without any active, positive steps delimiting how this use is actually practiced.

18. Claim 7 is indefinite because "and preferably all of them" (last 2 lines) is indefinite.

19. Claim 8 is indefinite because it is unclear what 'it' (line 2) is referring to. *For the purposes of this Office Action, 'it' is understood to refer to "the method" of claim 1.*

20. Claim 8 provides for the use of the method of claim 1, but, since the claim does not set forth any steps involved in the method/process, it is unclear what method/process applicant is intending to encompass. A claim is indefinite where it merely recites a use without any active, positive steps delimiting how this use is actually practiced.

21. Claim 8 is indefinite because it is unclear what "resulting from ..." is referring to.

22. Claim 8 recites the limitation "the one of the entities" in line 4. There is insufficient antecedent basis for this limitation in the claim. *For the purposes of this Office Action, "the one" is understood to be "one".*

Claim Rejections - 35 USC § 101

23. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

24. Claims 1-10 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Regarding claim 1, the claimed method is not tangibly embodied and has no tangible result.

25. Claims 6 & 8 are rejected under 35 U.S.C. 101 because the claimed recitation of a use, without setting forth any steps involved in the process, results in an improper definition of a process, i.e., results in a claim which is not a proper process claim under 35 U.S.C. 101. See for example *Ex parte Dunki*, 153 USPQ 678 (Bd.App. 1967) and *Clinical Products, Ltd.* v. *Brenner*, 255 F. Supp. 131, 149 USPQ 475 (D.D.C. 1966).

Claim Rejections - 35 USC § 103

26. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

27. Claim 1, as best understood, is rejected under 35 U.S.C. 103(a) as being unpatentable over "Fast Key Exchange with Elliptic Curve Systems" by Schroeppel et al. (Schroeppel), "A Public Key Cryptosystem Based on Elliptic Curves over Z/nZ Equivalent to Factoring" by Meyer et al. (Meyer), "Elliptic Curve Cryptosystems and Their Applications" by Koyama et al. (Koyama) and U.S. Patent 6,141,420 to Vanstone et al. (Vanstone). Schroeppel discloses a cryptographic method multiplying an odd order point/P of an elliptic curve/E by an integer/2 (doubling of P) (p. 2, ¶3), characterized in that, for exchanging information via the non-secure communication channel (Diffie-Hellman conversation), the above step includes addition/"double and add" (p. 2, ¶3) of points of said elliptic curve/E. Schroeppel lacks having of points on the curve. However, Meyer teaches that it is known to compute square roots during elliptic curve decryption (p. 54, §5). Further, Koyama teaches that halving, based on the Adleman-Manders-Miller algorithm, is used to compute square roots modulo an integer in elliptic curve cryptosystems (p. 53, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to compute a square root with a halving algorithm. One of ordinary skill in the art would have been motivated to perform such a modification to perform decryption based on elliptic curves, as taught by Meyer (p. 54, §5) and Koyama (p. 53, ¶1). As modified, Schroeppel lacks a non-supersingular elliptic curve. However, Vanstone teaches that non-supersingular curves are preferable to supersingular curves in elliptic curve cryptosystems because they are more robust (col. 14, lines 35-36). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a non-supersingular curve. One of ordinary skill in the art would have been motivated to perform such a modification to gain robustness, as taught by Vanstone (col. 14, lines 35-36).

28. Claim 8, as best understood, is rejected under 35 U.S.C. 103(a) as being unpatentable over Schroeppel, Meyer, Koyama and Vanstone, as applied to claim 1, in further view of "An Elliptic Curve Implementation of the Finite Field Digital Signature Algorithm" by Koblitz. Meyer, as modified above, lacks the digital signature algorithm as described in claim 8. However, Koblitz teaches ECDSA (the elliptic curve analogue of DSA, digital signature algorithm), which is about 12 times faster than standard DSA (p. 327). Koblitz teaches a signature protocol between two entities based on a pair of permanent keys belonging to one of the entities, one secret/ x and the other public/ Q, resulting from the scalar multiplication of the secret key/ x by another public key consisting of a point/ P of odd order r of a chosen non-supersingular elliptic curve E (p. 333, second half of the page). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to perform the digital signature algorithm with elliptic curves because it is 12 times faster, as taught by Koblitz (pp. 327 & 333).

Conclusion

29. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Specifically, "Field Inversion and Point Halving Revisited" by Fong et al. is cited for teaching "point halving" was independently developed by Knudsen and Schroeppel (¶1).

30. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841.

The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703)746-7239 (for formal communications intended for entry)
Or:
(571)273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
January 26, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100